UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/001,410	10/31/2001	George S. Gales	10017028-1	3057

7590   06/21/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

)

EXAMINER
SHERKAT, AREZOO

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 06/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	10/001,410	GALES ET AL.
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>31 October 2001</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>10/31/01&7/30/03</u>.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

Claims 1-27 are presented for examination.

Double Patenting

Claims 1-27 provisionally rejected under the judicially created doctrine of

obviousness-type double patenting as being unpatentable over claims 1-29 of

copending Application No. 10001431. Although the conflicting claims are not identical,

they are not patentably distinct from each other because the limitation "specifying a

remedy for the specified vulnerability" in the instant application is equivalent to the

limitation "specifying an action in response to detecting the specified network protocol

and data pattern".

This is a <u>provisional</u> obviousness-type double patenting rejection because the

conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-27 are rejected under 35 U.S.C. 102(e) as being anticipated by

Chefalas et al., (U.S. Publication No. 2002/0116639 and Chefalas hereinafter).

Regarding claims 12, 1, and 2, Chefalas discloses a method of defining the

security vulnerability of a computer system, comprising:

specifying an attack representing a recognized vulnerability of the computer

system, specifying at least one attribute of the specified attack (i.e., virus name),

specifying at least one policy definition with respect to detecting the vulnerability of the

specified attack (Page 4, Par. 0046); and

specifying a remedy for the specified vulnerability (Page 4, Par. 0047-0048).

Regarding claims 3 and 13, Chefalas discloses further comprising specifying a

computing platform of the computer system (Page 4, Par. 0047).

Regarding claims 4 and 14, Chefalas discloses further comprising:

specifying a security category of the specified attack, and specifying at least one

policy group with respect to the specified security category (Page 4, Par. 0046).

Regarding claims 5 and 15, Chefalas discloses further comprising specifying a

vulnerability scanner executing on the computer system (Page 2, Par. 0027-0028).

Regarding claims 6 and 16, Chefalas discloses wherein specifying at least one attribute of the specified attack comprises specifying an identification of the severity associated with a breach of the computer system by the attack (Page 5, Par. 0060).

Regarding claim 7, Chefalas discloses wherein specifying at least one attribute of the specified attack comprises specifying a description of the attack (Page 5, Par. 0060).

Regarding claims 8 and 17, Chefalas discloses wherein specifying at least one attribute of the specified attack comprises specifying an explanation of why the specified attack is important (i.e., to prevent the occurrence of this type of event in future)(Page 5, Par. 0059).

Regarding claims 9 and 18, Chefalas discloses wherein specifying at least one attribute of the specified attack comprises specifying how information is to be reported to a user with respect to the specified attack (i.e., notification to the manager, the administrator, or a technician)(Page 4, Par. 0047 and Page 5, Par. 0060).

Regarding claims 10, 19, and 27, Chefalas discloses wherein specifying at least one attribute of the specified attack comprises specifying a source of a remedy operable to fix the specified vulnerability (Page 5, Par. 0054-0058).

Regarding claim 11, Chefalas discloses wherein specifying at least one attribute
of the specified attack comprises specifying information to enable a manual remedy of
the specified vulnerability (Page 5, Par. 0060-0062).

Regarding claim 20, Chefalas discloses a system of defining security
vulnerabilities of a computer system, comprising:

vulnerability description file containing a definition of at least one vulnerability
(Fig. 4A, item 406), a definition of at least one policy item for the vulnerability (Fig. 4A,
item 408), an interpreter operable to parse the at least one vulnerability definition and at
least one policy item definition in the vulnerability description file and organize the
parsed definitions pursuant to a predetermined format, and a data storage operable to
store the parsed and organized at least one vulnerability and at least one policy item
definition, wherein the data storage is accessible by at least one vulnerability scanner
application (Page 4, Par. 0044-0048).

Regarding claim 21, Chefalas discloses wherein the data storage is a relational
database having a plurality of tables (Page 4, Par. 0046-0048).

Regarding claim 22, Chefalas discloses wherein the vulnerability description file
further comprises a definition of a vulnerability scanner application (i.e.,
instruction)(Page 4, Par. 0045).

Regarding claim 23, Chefalas discloses wherein the vulnerability description file further comprises a definition of a security category providing a grouping of the at least one vulnerability, and a definition of a policy group providing a grouping of the at least one policy item (Page 4, Par. 0046).

Regarding claim 24, Chefalas discloses wherein the vulnerability description file further comprises a definition of at least one attribute of the at least one vulnerability (i.e., virus name)(Page 4, Par. 0043-0044).

Regarding claim 25, Chefalas discloses wherein the vulnerability description file further comprises an identification of the severity of risk associated with the at least one vulnerability (Page 5, Par. 0060).

Regarding claim 26, Chefalas discloses wherein the vulnerability description file further comprises a definition of how information is to be displayed to a user with respect to the at least one vulnerability (i.e., notification to the manager, the administrator, or a technician)(Page 4, Par. 0047 and Page 5, Par. 0060).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Hartley et al., (U.S. Publication No. 2002/0026591),

Cooper et al. (U.S. Publication No. 2002/0053033),

Reshef et al., (U.S. Patent No. 6,584,569), and

Hill et al., (U.S. Patent No. 6,088,804).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Arezoo Sherkat
Patent Examiner
Group 2131
Jun 14, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100